REMARKS

Claims 1-17 have been rejected under 35 U.S.C. § 102(b) as anticipated by Williams (Published U.S. Patent Application No. 2003/0005331 A1). However, for the reasons discussed hereinafter, Applicants respectfully submit that independent Claim 1, and therefore all claims of record in this application, distinguish over Williams, whether considered by itself, or in combination with other references.

The present invention is directed to a method for secure communication between computer user domains which are connected by a "connecting network". As is known to those skilled in the art, a "domain" is a hierarchical organization of computers that enables multiple systems to communicate in a secure fashion. For example, computing systems frequently comprise user domains having different security classification networks, which domains are connected by the connecting network. In this case, it is necessary to protect data communicated between user domains of the same classification from unauthorized access (for example, unauthorized persons in user domains having a lower classification).

To this end, the present invention provides a method in which, before a data packet enters the connecting network from a user domain, two steps are performed: first, the data packet is tagged with a security level marking, and thereafter, the tagged data packet is appended with a string formed from a

check-sum made over the data packet and security level marking tag, to form a datagram. Thereafter, the datagram is transmitted among user domains by the connecting network. In order to be entered into a particular user domain, the following steps are performed: first, a check is made to verify that the string in the received datagram matches the string calculated over the received data packet and security level marking tag, and furthermore that the received security level marking tag matches the security level of the second user domain. If not, the data are discarded, and are not entered into the second user domain.

Unlike the present invention, the Williams patent application discloses a system involving security check devices that are attached to each computer in a computer network, together with a Network Security Computer (NSC), which administers the security devices. The security devices are interposed between each computer and the network, and check the security level of the data to be transmitted over the network, using a tag appended to the data by the computer, as described, for example, in paragraph [0053]. They also add a check-sum and then encrypt the data for transmission over the network. (Paragraphs [0189] – [0190].) At the receiving end, the respective security device decrypts the data and checks the security level of the data, discarding the data of the security level outside the permitted "security window", as discussed in paragraph [0196].

As can be seen from the foregoing brief descriptions, the method according to the present invention differs from that of Williams in at least one important

respect. That is, according to the present invention, as defined in Claim 1, the present invention needs only operate at the network level, such that the hardware which is required at each computer in Williams is unnecessary. Instead, the method according to the invention is performed at the domain level of a secure network.

Thus, Claim 1 defines a method of improving the security of computer communications "over a connecting network which consists of a plurality of user domains". To this end, a "data packet from a user domain" is tagged with a security level marking, and the same data packet (from a user domain) is appended with a string formed from a check-sum made over the data packet and the security level marking, to form a datagram. In this manner, the data packet can be sent to another domain having the corresponding security level, without concern that it will be entered into domains which are unauthorized, or which do not possess the requisite security level. That is, if the receiving network is appropriately cleared, it will be able to verify the received datagram, and to transmit the data onto the receiving secure network. If the datagram cannot be verified, however, the data are discarded.

Thus, the invention does not operate at the computer level, and does not require processing or hardware at the individual computer level. Rather, it is performed solely at the domain/network level. This arrangement provides the advantage that, within a secure network, the data can pass freely with no delay ,

and without need for expensive security devices, while at the same time maintaining the security of the data as it is transmitted over an unsecured network.

In light of the foregoing remarks, this application should be in condition for allowance, and early passage of this case to issue is respectfully requested. If there are any questions regarding this amendment or the application in general, a telephone call to the undersigned would be appreciated since this should expedite the prosecution of the application for all concerned.

If necessary to effect a timely response, this paper should be considered as a petition for an Extension of Time sufficient to effect a timely response, and please charge any deficiency in fees or credit any overpayments to Deposit Account No. 05-1323 (Docket #038665.56061US).

Respectfully submitted,

Gary R. Edwards
Registration No. 31,824

CROWELL & MORING LLP
Intellectual Property Group
P.O. Box 14300
Washington, DC 20044-4300
Telephone No.: (202) 624-2500
Facsimile No.: (202) 628-8844
GRE:kms
3040391_1